November 6, 2015

GAUSSIAN ELIMINATION IN SYMPLECTIC AND SPLIT ORTHOGONAL GROUPS

SUSHIL BHUNIA, AYAN MAHALANOBIS AND ANUPAM SINGH

IISER Pune, Dr. Homi Bhabha Road, Pashan, Pune 411008, INDIA.

ABSTRACT. This paper studies algorithms similar to the Gaussian elimination algorithm in symplectic and split orthogonal groups. We discuss two applications of this algorithm in computational group theory. One computes the spinor norm and the other computes the double coset decomposition with respect to Siegel maximal parabolic subgroup.

1. INTRODUCTION

Gaussian elimination is a very old theme in Mathematics. It appeared in print as chapter eight in a Chinese mathematical text called, "The nine chapters of the mathematical art". It is believed, a part of that book was written as early as 150 BCE. For a historical perspective on Gaussian elimination, we refer to a nice work by Grcar [9].

Due to many reasons [19], computational group theorists became interested in the *constructive group recognition project*. We will not go in any details of this project, but will refer an interested reader to the works of Leedham-Green and O'Brein [13] and O'Brein [18, Section 9]. One can also read a nice but slightly outdated review by Seress [20, Matrix Groups] in this context. In dealing with constructive group recognition, one needs to solve the *word problem* in some generating set. As we know, in the special linear group $\mathrm{SL}(d,k)$, the word problem has an efficient solution in elementary transvections – Gaussian elimination.

In this paper, we work with Chevalley generators [4, §11.3]. Chevalley generators for the special linear group are elementary transvections. These Chevalley generators for other classical groups are known for a very long time. However, its use in row-column operations in symplectic and split orthogonal groups is new. We develop row-column operations, very similar to the Gaussian elimination algorithm for special linear groups. We call our algorithms Gaussian elimination in symplectic and split orthogonal groups respectively. Similar algorithm for twisted orthogonal groups and unitary groups [14] are being developed.

The current trend in *computational group theory* is to use *standard generators*. Using standard generators, Brooksbank [3], Costi [8] solves the word problem in classical groups and Ambrose et. al. [1] solves the membership problem in black-box groups. One advantage of using standard generators is that they are few in number. However, there is a disadvantages in working with them – they only work in finite fields. While working with Chevalley generators, our algorithms have two advantages:

1. It works for arbitrary fields.
2. It is much more efficient, as we demonstrate with an actual implementation in Magma [2], see Figures 1 & 2.

E-mail address: sushilbhunia@gmail.com, ayan.mahalanobis@gmail.com, anupamk18@gmail.com.

2010 *Mathematics Subject Classification.* 20H20, 68W30.

This work is supported by a SERB research grant.

From our algorithm, one can compute the spinor norm easily, see Section 5.2. Murray and Roney-Dougal [16] studied computing spinor norm earlier. Our algorithm can also be used to compute the double coset decomposition corresponding to the Siegel maximal parabolic subgroup, see Section 6.

Algorithms that we develop in this paper work only for a given bilinear form β(see Equations 2.2, 2.1). Our algorithm work well on all characteristics for symplectic groups. However, for orthogonal groups our algorithms work only for odd characteristic. Henceforth, by **suitable characteristics** we mean all characteristics for the symplectic groups and zero or odd characteristic for orthogonal groups. It is known, in a field of suitable characteristics, all non-degenerate skew-symmetric bilinear forms are equivalent and all split (maximal Witt index) symmetric bilinear forms are equivalent. These equivalent bilinear forms are obtained by a base-change matrix and gives rise to conjugate linear groups. Though in our algorithm, we work with only one bilinear form β, given by a fixed basis, with a suitable change of basis matrix our algorithm works on any equivalent bilinear forms.

Another way to look at this paper, we have an algorithmic proof of this well-known theorem. For definitions of elementary matrices, one can look ahead to Section 3.

Theorem A. *Let k be a field of suitable characteristic. For $d \geq 4$ or $l \geq 2$ following holds:*

($\mathscr{A}$) *Every element of the split orthogonal group $O(d,k)$ can be written as a product of elementary matrices and a diagonal matrix. Furthermore, the diagonal matrix is of the form*

$$\begin{aligned} &\operatorname{diag}(1,\ldots,1,\lambda,1,\ldots,1,\lambda^{-1}) && \lambda \in k^{\times} && \text{whenever } d = 2l \\ &\operatorname{diag}(\vartheta,1,\ldots,1,\lambda,1,\ldots,1,\lambda^{-1}) && \lambda \in k^{\times} \text{ and } \vartheta = \pm 1 && \text{whenever } d = 2l+1. \end{aligned}$$

($\mathscr{B}$) *Every element of the symplectic group $Sp(2l,k)$ can be written as a product of elementary matrices.*

This theorem has a surprising corollary. It follows that:

Corollary B. *In an orthogonal group, the image of λ in $k^{\times}/k^{\times 2}$ is the spinor norm.*

This means that we have an efficient algorithm to compute the spinor norm. Since the commutator subgroup of the orthogonal group is the kernel of the spinor norm restricted to special orthogonal group, the above corollary is a membership test for the commutator subgroup in the orthogonal group. In other words, an element g in the special orthogonal group belongs to the commutator subgroup if and only if the λ it produces in the Gaussian elimination algorithm is a square in the field, see Equation 2.3.

The bilinear form that we use and the generators that we define have its roots in the abstract root system of a semisimple Lie algebra and Chevalley groups defined by Chevalley and Steinberg [6, 21]. However we assume no knowledge of Lie theory or Chevalley groups in this paper.

2. Orthogonal and Symplectic Groups

We begin with a brief introduction of orthogonal and symplectic groups. We follow Carter [4], Taylor [22] and Grove [10] in our introduction. In this section, we **fix some notations** which will be used throughout this paper. We denote the transpose of a matrix X by ${}^{T}X$.

Let V be a vector space of dimension d over a field k of suitable characteristic. Let $\beta : V \times V \to k$ be a bilinear form. By fixing a basis of V we can associate a matrix to β. We shall abuse the notation slightly and denote the matrix of the bilinear form by β itself. Thus $\beta(x,y) = {}^{T}x\beta y$ where x, y are column vectors. We will work with non-degenerate bilinear forms, which implies, $\det\beta \neq 0$. A symmetric or skew-symmetric bilinear form β satisfies $\beta = {}^{T}\beta$ or $\beta =$

$-^T\beta$ respectively. In even order, for characteristic 2, the symmetric and skew-symmetric forms are the same.

Definition 2.1 (Orthogonal Groups)**.** *A square matrix X of size d is called orthogonal if ${}^TX\beta X = \beta$ where β is symmetric. The set of orthogonal matrices form the orthogonal group.*

In this paper, we deal with the split orthogonal group defined by one particular bilinear form defined over a field of zero or odd characteristics in Equations 2.2. So any mention of orthogonal group means this one particular orthogonal group, unless stated otherwise.

Definition 2.2 (Symplectic Group)**.** *A square matrix X of size d is called symplectic if ${}^TX\beta X = \beta$ where β is skew-symmetric. The set of symplectic matrices form the symplectic group.*

In this paper, we deal with the symplectic group defined by the bilinear form defined by Equation 2.1. So any mention of symplectic group means this one particular symplectic group, unless stated otherwise.

We write the dimension of V as d where $d = 2l+1$ or $d = 2l$ and $l \geq 1$. In the case β is symmetric we define the corresponding quadratic form $Q\colon V \to k$ by $Q(v) = \frac{1}{2}\beta(v,v)$. Up to equivalence, there is an unique non-degenerate skew-symmetric bilinear form over a field k of suitable characteristics. Furthermore a skew-symmetric bilinear form exists only in even dimension. We fix a basis of V as $\{e_1,\ldots,e_l,e_{-1},\ldots,e_{-l}\}$ so that the matrix β is:

$$\beta = \begin{pmatrix} 0 & I_l \\ -I_l & 0 \end{pmatrix}. \tag{2.1}$$

The symplectic group with this β is denoted by $\mathrm{Sp}(2l,k)$.

Up to equivalence, there is a unique non-degenerate symmetric bilinear form of maximal Witt index over a field k of suitable characteristics. This is also called the split form. We fix a basis $\{e_0,e_1,\ldots,e_l,e_{-1},\ldots,e_{-l}\}$ for odd dimension and $\{e_1,\ldots,e_l,e_{-1},\ldots,e_{-l}\}$ for even dimension so that the matrix β is:

$$\beta = \begin{cases} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & I_l \\ 0 & I_l & 0 \end{pmatrix} & \text{when } d = 2l+1 \\ \begin{pmatrix} 0 & I_l \\ I_l & 0 \end{pmatrix} & \text{when } d = 2l. \end{cases} \tag{2.2}$$

The orthogonal group corresponding to this form is a *split orthogonal group*. In this paper, we will simply call it *the orthogonal group* and this group will be denoted by $\mathrm{O}(d,k)$. If we need to emphasize parity of the dimension, we will write $\mathrm{O}(2l+1,k)$ or $\mathrm{O}(2l,k)$. We denote by $\Omega(d,k)$ the commutator subgroup of the orthogonal group $\mathrm{O}(d,k)$ which is equal to the commutator subgroup of $\mathrm{SO}(d,k)$. There is a well known exact sequence

$$1 \longrightarrow \Omega(d,k) \longrightarrow \mathrm{SO}(d,k) \xrightarrow{\Theta} k^\times/k^{\times 2} \longrightarrow 1 \tag{2.3}$$

where Θ is the spinor norm. The spinor norm is defined as $\Theta(g) = \prod_{i=1}^{m} Q(v_i)$ where $g = \rho_{v_1}\cdots\rho_{v_m}$ is written as a product of reflections. Since the group $\mathrm{SO}(d,k)$ is of index 2 in $\mathrm{O}(d,k)$, we fix a generator for the quotient as $w_l = I - e_{l,l} - e_{-l,-l} - e_{l,-l} - e_{-l,l}$.

3. Elementary Matrices and Elementary Operations

In what follows, the scalar t varies over the field k and $1 \leq i,j \leq l$. Furthermore, $l \geq 2$ which means $d \geq 4$. We define $te_{i,j}$ as the matrix unit with t in the (i,j) position and zero everywhere else. We use $e_{i,j}$ to denote $1e_{i,j}$. We often use the well known identity $e_{i,j}e_{k,l} = \delta_{j,k}e_{i,l}$ where $\delta_{i,j}$ is the Kronecker delta.

3.1. **Elementary Matrices for $\mathbf{O}(2l,k)$.** We index rows by $1,2,\ldots,l,-1,-2,\ldots,-l$. The elementary matrices are defined as follows:

$$\begin{aligned} x_{i,j}(t) &= I + t(e_{i,j} - e_{-j,-i}) && \text{for } i \neq j, \\ x_{i,-j}(t) &= I + t(e_{i,-j} - e_{j,-i}) && \text{for } i < j, \\ x_{-i,j}(t) &= I + t(e_{-i,j} - e_{-j,i}) && \text{for } i < j, \\ w_l &= I - e_{l,l} - e_{-l,-l} - e_{l,-l} - e_{-l,l} \end{aligned}$$

and in matrix format

E1: $\begin{pmatrix} R & 0 \\ 0 & {}^{T}R^{-1} \end{pmatrix}$ where $R = I + te_{i,j}$; $i \neq j$

E2: $\begin{pmatrix} I & R \\ 0 & I \end{pmatrix}$ where R is $t(e_{i,j} - e_{j,i})$ for $i < j$

E3: $\begin{pmatrix} I & 0 \\ R & I \end{pmatrix}$ where R is $t(e_{i,j} - e_{j,i})$ for $i < j$.

The row and column operations:

$$\begin{aligned} ER1: \quad & \begin{pmatrix} R & 0 \\ 0 & {}^{T}R^{-1} \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} RA & RB \\ {}^{T}R^{-1}C & {}^{T}R^{-1}D \end{pmatrix} \\ EC1: \quad & \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} R & 0 \\ 0 & {}^{T}R^{-1} \end{pmatrix} = \begin{pmatrix} AR & B^{T}R^{-1} \\ CR & D^{T}R^{-1} \end{pmatrix}. \end{aligned}$$

$$\begin{aligned} ER2: \quad & \begin{pmatrix} I & R \\ 0 & I \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A + RC & B + RD \\ C & D \end{pmatrix} \\ EC2: \quad & \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} I & R \\ 0 & I \end{pmatrix} = \begin{pmatrix} A & AR + B \\ C & CR + D \end{pmatrix}. \end{aligned}$$

$$\begin{aligned} ER3: \quad & \begin{pmatrix} I & 0 \\ R & I \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A & B \\ RA + C & RB + D \end{pmatrix} \\ EC3: \quad & \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} I & 0 \\ R & I \end{pmatrix} = \begin{pmatrix} A + BR & B \\ C + DR & D \end{pmatrix}. \end{aligned}$$

3.2. **Elementary Matrices for $\mathbf{O}(2l+1,k)$.** We index rows by $0,1,\ldots,l,-1,\ldots,-l$. The elementary matrices are:

$$\begin{aligned} x_{i,j}(t) &= I + t(e_{i,j} - e_{-j,-i}) && \text{for } i \neq j, \\ x_{i,-j}(t) &= I + t(e_{i,-j} - e_{j,-i}), && \text{for } i < j, \\ x_{-i,j}(t) &= I + t(e_{-i,j} - e_{-j,i}) && \text{for } i < j, \\ x_{i,0}(t) &= I + t(2e_{i,0} - e_{0,-i}) - t^2 e_{i,-i}, \\ x_{0,i}(t) &= I + t(-2e_{-i,0} + e_{0,i}) - t^2 e_{-i,i}. \end{aligned}$$

Written in matrix format, these four kind of elementary matrices are:

E1: $\begin{pmatrix} 1 & 0 & 0 \\ 0 & R & 0 \\ 0 & 0 & {}^{T}R^{-1} \end{pmatrix}$ where $R = I + te_{i,j}$; $i \neq j$.

E2: $\begin{pmatrix} 1 & 0 & 0 \\ 0 & I & R \\ 0 & 0 & I \end{pmatrix}$ where R is $t(e_{i,j} - e_{j,i})$; $i < j$.

E3: $\begin{pmatrix} 1 & 0 & 0 \\ 0 & I & 0 \\ 0 & R & I \end{pmatrix}$ where R is $t(e_{i,j}-e_{j,i})$; $i<j$.

E4a: $\begin{pmatrix} 1 & 0 & R \\ -2R & I & -{}^TRR \\ 0 & 0 & I \end{pmatrix}$ where $R=te_i$

E4b: $\begin{pmatrix} 1 & R & 0 \\ 0 & I & 0 \\ -2R & -{}^TRR & I \end{pmatrix}$ where $R=te_i$

Here e_i is the row vector with 1 at i^{th} place and zero elsewhere.

3.3. **Elementary operations for $\mathbf{O}(2l+1,k)$.** Let $g=\begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix}$ be a $(2l+1)\times(2l+1)$ matrix where A,B,C,D are $l\times l$ matrices. The matrices $X=(X_1,X_2,\ldots,X_l)$, $Y=(Y_1,Y_2,\ldots,Y_l)$, $E={}^T(E_1,E_2,\ldots,E_l)$ and $F={}^T(F_1,F_2,\ldots,F_l)$. Let $\alpha\in k$. Let us note the effect of multiplication by elementary matrices from above.

$$ER1:\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & R & 0 \\ 0 & 0 & {}^TR^{-1} \end{pmatrix}\begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix} = \begin{pmatrix} \alpha & X & Y \\ RE & RA & RB \\ {}^TR^{-1}F & {}^TR^{-1}C & {}^TR^{-1}D \end{pmatrix}$$

$$EC1:\ \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & R & 0 \\ 0 & 0 & {}^TR^{-1} \end{pmatrix} = \begin{pmatrix} \alpha & XR & Y{}^TR^{-1} \\ E & AR & B{}^TR^{-1} \\ F & CR & D{}^TR^{-1} \end{pmatrix}.$$

$$ER2:\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & I & R \\ 0 & 0 & I \end{pmatrix}\begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix} = \begin{pmatrix} \alpha & X & Y \\ E+RF & A+RC & B+RD \\ F & C & D \end{pmatrix}$$

$$EC2:\ \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & I & R \\ 0 & 0 & I \end{pmatrix} = \begin{pmatrix} \alpha & X & XR+Y \\ E & A & AR+B \\ F & C & CR+D \end{pmatrix}.$$

$$ER3:\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & I & 0 \\ 0 & R & I \end{pmatrix}\begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix} = \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ RE+F & RA+C & RB+D \end{pmatrix}$$

$$EC3:\ \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & I & 0 \\ 0 & R & I \end{pmatrix} = \begin{pmatrix} \alpha & X+YR & Y \\ E & A+BR & B \\ F & C+DR & D \end{pmatrix}.$$

For E4 we only write the equations that we need later.

- Let the matrix g has $C=\operatorname{diag}(d_1,\ldots,d_l)$.

$$ER4:\ [(I+te_{0,-i}-2te_{i,0}-t^2e_{i,-i})g]_{0,i}=X_i+td_i$$

$$EC4:\ [g(I+te_{0,-i}-2te_{i,0}-t^2e_{i,-i})]_{-i,0}=F_i-2td_i.$$

- Let the matrix g has $A=\operatorname{diag}(d_1,\ldots,d_l)$.

$$ER4:\ [(I+te_{0,i}-2te_{-i,0}-t^2e_{-i,i})g]_{0,i}=X_i+td_i$$

$$EC4:\ [g(I+te_{0,-i}-2te_{i,0}-t^2e_{i,-i})]_{i,0}=E_i-2td_i.$$

3.4. **Elementary Matrices for $\mathbf{Sp}(2l,k)$.**

$$\begin{aligned} x_{i,j}(t) &= I + t(e_{i,j} - e_{-j,-i}) \quad \text{for } i \neq j, \\ x_{i,-j}(t) &= I + t(e_{i,-j} + e_{j,-i}) \quad \text{for } i < j, \\ x_{-i,j}(t) &= I + t(e_{-i,j} + e_{-j,i}) \quad \text{for } i < j, \\ x_{i,-i}(t) &= I + te_{i,-i} \\ x_{-i,i}(t) &= I + te_{-i,i}. \end{aligned}$$

There are three kinds of elementary matrices.

E1: $\begin{pmatrix} R & 0 \\ 0 & {}^{T}R^{-1} \end{pmatrix}$ where $R = I + te_{i,j}$; $i \neq j$.

E2: $\begin{pmatrix} I & R \\ 0 & I \end{pmatrix}$ where R is either $t(e_{i,j} + e_{j,i})$; $i < j$ or $te_{i,i}$.

E3: $\begin{pmatrix} I & 0 \\ R & I \end{pmatrix}$ where R is either $t(e_{i,j} + e_{j,i})$; $i < j$ or $te_{i,i}$.

3.5. **Elementary Operations for $\mathbf{Sp}(2l,k)$.** Let $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ be a $2l \times 2l$ matrix written in block form of size $l \times l$. Then the row and column operations are as follows:

$$\begin{aligned} ER1: \quad \begin{pmatrix} R & 0 \\ 0 & {}^{T}R^{-1} \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} &= \begin{pmatrix} RA & RB \\ {}^{T}R^{-1}C & {}^{T}R^{-1}D \end{pmatrix} \\ EC1: \quad \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} R & 0 \\ 0 & {}^{T}R^{-1} \end{pmatrix} &= \begin{pmatrix} AR & B^{T}R^{-1} \\ CR & D^{T}R^{-1} \end{pmatrix}. \end{aligned}$$

$$\begin{aligned} ER2: \quad \begin{pmatrix} I & R \\ 0 & I \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} &= \begin{pmatrix} A + RC & B + RD \\ C & D \end{pmatrix} \\ EC2: \quad \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} I & R \\ 0 & I \end{pmatrix} &= \begin{pmatrix} A & AR + B \\ C & CR + D \end{pmatrix}. \end{aligned}$$

$$\begin{aligned} ER3: \quad \begin{pmatrix} I & 0 \\ R & I \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} &= \begin{pmatrix} A & B \\ RA + C & RB + D \end{pmatrix} \\ EC3: \quad \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} I & 0 \\ R & I \end{pmatrix} &= \begin{pmatrix} A + BR & B \\ C + DR & D \end{pmatrix}. \end{aligned}$$

Remark: We would require row-interchange of i^{th} row with $-i^{\text{th}}$ row in our algorithms. In the case of symplectic and odd-order orthogonal groups this row-interchange is a product of elementary matrices. In the case of even-order orthogonal groups, we need to add to generators a row-interchange matrix w_l. For more see Lemma 4.6.

4. Gaussian Elimination in orthogonal and symplectic groups

Recall the field k is of suitable characteristic. Cohen, Murray and Taylor [7] proposed a generalized row-column operations, using a representation of Chevalley groups. The key idea there was to bring down an element to a maximal parabolic subgroup and repeat the process inductively. The emphasis there was to represent generators as symbols so that it takes less memory to store. Here we use the natural matrix representation of these groups.

4.1. **Gaussian Elimination for $\mathbf{Sp}(2l,k)$ and $\mathbf{O}(2l,k)$.** The algorithm is as follows.

Step 1: **Input**: A matrix $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ which belongs to $\mathrm{Sp}(2l,k)$ or $\mathrm{O}(2l,k)$.

Output: The matrix $g_1 = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}$ is one of the following kind:

a: The matrix A_1 is a diagonal matrix $\mathrm{diag}(1,\ldots,1,\lambda)$ with $\lambda \neq 0$ and C_1 is $\begin{pmatrix} C_{11} & C_{12} \\ C_{21} & c_{22} \end{pmatrix}$ where C_{11} is symmetric when g is in $\mathrm{Sp}(2l,k)$ and skew-symmetric when g is in $\mathrm{O}(2l,k)$ and is of size $l-1$. Furthermore, $C_{12} = \lambda^T C_{21}$ when g is in $\mathrm{Sp}(2l,k)$ and $C_{12} = -\lambda^T C_{21}$, $c_{22} = 0$ when g is in $\mathrm{O}(2l,k)$.

b: The matrix A_1 is a diagonal matrix $\mathrm{diag}(1,\ldots,1,0,\ldots,0)$ with number of 1s equal to m and C_1 is of the form $\begin{pmatrix} C_{11} & 0 \\ C_{21} & C_{22} \end{pmatrix}$ where C_{11} is an $m \times m$ symmetric matrix when g is in $\mathrm{Sp}(2l,k)$ and skew-symmetric when g is in $\mathrm{O}(2l,k)$.

Justification: Observe the effect of ER1 and EC1 on the block A. This amounts to Gaussian elimination on a $l \times l$ matrix. Thus we can reduce A to a diagonal matrix and Corollary 4.2 makes sure that C has required form.

Step 2: **Input:** matrix $g_1 = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}$.

Output: matrix $g_2 = \begin{pmatrix} A_2 & B_2 \\ 0 & {}^T A_2^{-1} \end{pmatrix}$; A_2 is a diagonal matrix $\mathrm{diag}(1,\ldots,1,\lambda)$.

Justification: Observe the effect of ER3. It changes C_1 to $RA_1 + C_1$. Using Lemma 4.5 we can make the matrix C_1 the zero matrix in the first case and C_{11} the zero matrix in the second case. Furthermore, in the second case, we use Lemma 4.6 to interchange the rows so that we get the zero matrix in the place of C_1. If required use ER1 and EC1 to make A_1 a diagonal matrix. Lemma 4.4 ensures that D_1 becomes ${}^T A_2^{-1}$.

Step 3: **Input:** matrix $g_2 = \begin{pmatrix} A_2 & B_2 \\ 0 & {}^T A_2^{-1} \end{pmatrix}$; A_2 is a diagonal matrix $\mathrm{diag}(1,\ldots,1,\lambda)$.

Output: Matrix $g_3 = \begin{pmatrix} A_2 & 0 \\ 0 & {}^T A_2^{-1} \end{pmatrix}$; A_2 is diagonal matrix $\mathrm{diag}(1,\ldots,1,\lambda)$.

Justification: Using Corollary 4.3 we see that the matrix B_2 has certain form. We can use ER2 to make the matrix B_2 a zero matrix because of Lemma 4.5.

The algorithm terminates here for $\mathrm{O}(2l,k)$. However for $\mathrm{Sp}(2l,k)$ there is one more step.

Step 4: **Input:** matrix $g_3 = \mathrm{diag}(1,\ldots,1,\lambda,1,\ldots,1,\lambda^{-1})$.

Output: Identity matrix

Justification: This can be written as a product of elementary matrices by the first part of Lemma 4.7.

4.2. **Gaussian Elimination for $\mathbf{O}(2l+1,k)$.** An overview of the algorithm is as follows:

Step 1: **Input:** matrix $g = \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix}$ which belongs to $\mathrm{O}(2l+1,k)$;

Output: matrix $g_1 = \begin{pmatrix} \alpha & X_1 & Y_1 \\ E_1 & A_1 & B_1 \\ F_1 & C_1 & D_1 \end{pmatrix}$ of one of the following kind:

a: The matrix A_1 is a diagonal matrix $\mathrm{diag}(1,\ldots,1,\lambda)$ with $\lambda \neq 0$.

b: The matrix A_1 is a diagonal matrix $\mathrm{diag}(1,\ldots,1,0,\ldots,0)$ with number of 1s equal to m and $m < l$.

Justification: Using ER1 and EC1 we do the classical Gaussian elimination on a $l \times l$ matrix A.

Step 2: **Input:** matrix $g_1 = \begin{pmatrix} \alpha & X_1 & Y_1 \\ E_1 & A_1 & B_1 \\ F_1 & C_1 & D_1 \end{pmatrix}$.

Output: matrix $g_2 = \begin{pmatrix} \alpha_2 & X_2 & Y_2 \\ E_2 & A_2 & B_2 \\ F_2 & C_2 & D_2 \end{pmatrix}$ of one of the following kind:

a: The matrix A_2 is $\text{diag}(1,1,\ldots,1,\lambda)$ with $\lambda \neq 0$, $X_2 = 0 = E_2$ and C_2 is of the form $\begin{pmatrix} C_{11} & -\lambda^T C_{21} \\ C_{21} & 0 \end{pmatrix}$ where C_{11} is skew-symmetric of size $l-1$.

b: The matrix A_2 is $\text{diag}(1,\ldots,1,0,\ldots,0)$ with number of 1s equal to m; X_2 and E_2 have first m entries 0, and C_2 is of the form $\begin{pmatrix} C_{11} & 0 \\ C_{21} & C_{22} \end{pmatrix}$ where C_{11} is an $m \times m$ skew-symmetric.

Justification: Once we have A_1 in diagonal form we use ER4 and EC4 to change X_1 and E_1 in the required form. Then Lemma 4.8 makes sure that C_1 has required form.

Step 3: **Input:** matrix $g_2 = \begin{pmatrix} \alpha_2 & X_2 & Y_2 \\ E_2 & A_2 & B_2 \\ F_2 & C_2 & D_2 \end{pmatrix}$.

Output:

a: matrix $g_3 = \begin{pmatrix} \alpha_3 & 0 & Y_3 \\ 0 & A_3 & B_3 \\ F_3 & 0 & D_3 \end{pmatrix}$ where A_3 is $\text{diag}(1,1,\ldots,1,\lambda)$.

b: matrix $g_3 = \begin{pmatrix} \alpha_3 & X_3 & Y_3 \\ E_3 & A_3 & B_3 \\ F_3 & C_3 & D_3 \end{pmatrix}$ where A_3 is $\text{diag}(1,\ldots,1,0,\ldots,0)$ with number of 1s equal to m; X_3 and E_3 have first m entries 0, and C_3 is of the form $\begin{pmatrix} 0 & 0 \\ C_{21} & C_{22} \end{pmatrix}$.

Justification: Observe the effect of ER3 and the Lemma 4.5 ensures the required form.

Step 4: **Input:** $g_3 = \begin{pmatrix} \alpha_3 & X_3 & Y_3 \\ E_3 & A_3 & B_3 \\ F_3 & C_3 & D_3 \end{pmatrix}$.

Output: $g_4 = \begin{pmatrix} \vartheta & 0 & 0 \\ 0 & A_4 & B_4 \\ 0 & 0 & A_4^{-1} \end{pmatrix}$ with A_4 diagonal matrix $\text{diag}(1,\ldots,1,\lambda)$.

Justification: In the first case, Lemma 4.10 ensures the result. In the second case we interchange i^{th} with $-i^{\text{th}}$ for $m+1 \leq i \leq l$. This will make $C_3 = 0$. Then if needed we use ER1 and EC1 on A_3 to make it a diagonal. Lemma 4.9 ensures that A_3 has full rank. Furthermore, we can use ER4 and EC4 to make $X_3 = 0$ and $E_3 = 0$. Lemma 4.10 gives the required form.

Step 5: **Input:** $g_4 = \begin{pmatrix} \vartheta & 0 & 0 \\ 0 & A_4 & B_4 \\ 0 & 0 & A_4^{-1} \end{pmatrix}$ with $A_4 = \text{diag}(1,\ldots,1,\lambda)$.

Output: $g_5 = \text{diag}(\vartheta, 1\ldots,1,\lambda,1,\ldots,1,\lambda^{-1})$.

Justification: Lemma 4.10 ensures that B_4 is of certain kind. Use ER2 to make $B_4 = 0$. Lemma 4.6 ensures that the first diagonal entry is ϑ.

Proof of the Theorem A. ($\mathscr{A}$) Let $g \in \mathrm{O}(d,k)$. Using the above algorithm we can reduce g to a diagonal matrix of the required form.

($\mathscr{B}$) If $g \in \mathrm{Sp}(2l,k)$ using above algorithm and Lemma 4.7 we can reduce g to the identity. Thus g is a product of elementary matrices.

•

This algorithm can be used to compute the determinant of an orthogonal group. In the even-order case, refer to Algorithm 4.1. After Step 1, either A_1 has full rank, or the rank of A_1 is m. In the first case the determinant of g is 1 and in the second case it is $(-1)^{l-m}$. It is fairly straightforward to see this. Observe that all elementary matrix other than the row-interchange matrix has determinant one and the number of row-interchange that we do is $l-m$, where m is the rank of A_1.

In the odd-order case, as we have observed that the row-interchange matrix is a product of elementary matrices and all elementary matrices have determinant one. It then follows clearly that the determinant of g is ϑ.

4.3. **Time-complexity of the above algorithm.** We establish that the worst case time-complexity of the above algorithm is $\mathrm{O}(l^3)$.

In Step 1, we make A a diagonal matrix by row-column operations. That has complexity $\mathrm{O}(l^3)$.

In Step 2, $C_1 + RA_1$ is multiplying two rows by a field element and two additions. In the worst case, it has to be done $O(l)$ times and done $O(l^2)$ many times. So the complexity is $\mathrm{O}(l^3)$.

Step 3 is similar to Step 2 above and has complexity $\mathrm{O}(l^3)$.

Step 4 has only a few steps that is independent of l.

Then clearly, the time-complexity of our algorithm is $\mathrm{O}(l^3)$.

4.4. **Lemmas used in the justification of the Gaussian elimination.** To justify the steps of Gaussian algorithm we need several lemmas. Some of these might be well known to experts but we include them here for the convenience of the reader.

Lemma 4.1. *Let $Y = \mathrm{diag}(1,\ldots,1,\lambda,\ldots,\lambda)$ be of size l with number of 1s equal to $m < l$. Let X be a matrix of size $2l$ such that YX is symmetric (skew-symmetric) then X is of the form $\begin{pmatrix} X_{11} & \lambda^T X_{21} \\ X_{21} & X_{22} \end{pmatrix}$ where X_{11} is symmetric (skew symmetric) and $X_{12} = \lambda^T X_{21}$ ($X_{12} = -\lambda^T X_{21}$). Furthermore, if $\lambda \neq 0$ then X_{22} is symmetric (skew-symmetric).*

Proof. We observe that the matrix $YX = \begin{pmatrix} X_{11} & X_{12} \\ \lambda X_{21} & \lambda X_{22} \end{pmatrix}$. The condition that YX is symmetric implies X_{11} (and X_{22} if $\lambda \neq 0$) is symmetric and $X_{12} = \lambda^T X_{21}$. •

Corollary 4.2. *Let $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ be either in $Sp(2l,k)$ or $O(2l,k)$.*

(1) *If A is a diagonal matrix $\mathrm{diag}(1,\ldots,1,0,\ldots,0)$ with number of 1s equal to $m(<l)$ then the matrix C is $\begin{pmatrix} C_{11} & 0 \\ C_{21} & c_{22} \end{pmatrix}$ where C_{11} is an $m \times m$ symmetric if g is symplectic and is skew-symmetric if g is orthogonal.*

(2) *If A is a diagonal matrix $\mathrm{diag}(1,1,\ldots,1,\lambda)$ then the matrix C is $\begin{pmatrix} C_{11} & \lambda^T C_{21} \\ C_{21} & c_{22} \end{pmatrix}$ where C_{11} is an $(l-1)\times(l-1)$ symmetric if g is symplectic and C_{11} is skew-symmetric with $c_{22} = 0$ if g is orthogonal.*

Proof. We use the condition that g satisfies ${}^T g\beta g = \beta$ and get AC is symmetric (using $A = {}^T A$ as A is diagonal) when g is symplectic and skew-symmetric when g is orthogonal. The Lemma 4.1 gives the required form for C. •

Corollary 4.3. *Let* $g = \begin{pmatrix} A & B \\ 0 & A^{-1} \end{pmatrix}$ *where* $A = \mathrm{diag}(1,\ldots,1,\lambda)$ *be an element of either* $Sp(2l,k)$ *or* $O(2l,k)$ *then the matrix* B *is of the form* $\begin{pmatrix} B_{11} & \pm\lambda^{-1}{}^T B_{21} \\ B_{21} & B_{22} \end{pmatrix}$ *where* B_{11} *is a symmetric matrix of size* $l-1$ *if* g *is symplectic and is skew-symmetric along with* $B_{22} = 0$ *if* g *is orthogonal.*

Proof. Yet again, we use the condition that g satisfies ${}^T g\beta g = \beta$ and $A = {}^T A$ to get $A^{-1}B$ is symmetric if g is symplectic and is skew-symmetric if g is orthogonal. Then Lemma 4.1 gives the required form for B. •

Lemma 4.4. *Let* $g = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in GL(2l,k)$. *Then,*

(1) *the element* g *belongs to* $Sp(2l,k)$ *if and only if* $D = {}^T A^{-1}$ *and* $BA = A^T B$ *and*
(2) *the element* g *belongs to* $O(2l,k)$ *if and only if* $D = {}^T A^{-1}$ *and* $BA = -A^T B$.

Proof. This follows by simple computation using ${}^T g\beta g = \beta$. •

Lemma 4.5. *Let* $Y = \mathrm{diag}(1,1,\ldots,1,\lambda)$ *be of size* l *where* $\lambda \neq 0$ *and* $X = (x_{ij})$ *be a matrix such that* YX *is symmetric (skew-symmetric). Then* $X = (R_1 + R_2 + \ldots)Y$ *where each* R_m *is of the form* $t(e_{i,j} + e_{j,i})$ *for some* $i < j$ *or of the form* $te_{i,i}$ *for some* i *(in the case of skew-symmetric each* R_m *is of the form* $t(e_{i,j} - e_{j,i})$ *for some* $i < j$*).*

Proof. Since YX is symmetric, the matrix X is of the form $\begin{pmatrix} X_{11} & X_{12} \\ X_{21} & x_{ll} \end{pmatrix}$ where X_{11} is symmetric and X_{21} is a row of size $l-1$ and $X_{12} = \lambda {}^T X_{21}$. Clearly any such matrix is sum of the matrices of the form $R_m Y$. A similar calculation proves the result for the skew-symmetric case. •

We need certain Weyl group elements which can be used for interchanging rows. We use a formula $w_r = x_r(1)x_{-r}(-1)x_r(1)$ from the theory of Chevalley groups [4, Lemma 6.4.4] and construct elements $w_{i,j}$ and $w_{i,-j}$. In our algorithm, we need elements which interchanges i^{th} row with $-i^{\text{th}}$ row for any i. The element $w_{i,-i}$ that we create when multiplied to a matrix g interchanges its rows while simultaneously multiplying some rows by -1. However that does no harm to our algorithm.

Lemma 4.6. *For* $1 \leq i \leq l$,

(1) *the element* $w_{i,-i} = I + e_{i,-i} - e_{-i,i} - e_{i,i} - e_{-i,-i} \in Sp(2l,k)$ *is a product of elementary matrices.*
(2) *the element* $w_{i,-i} = I - 2e_{0,0} - e_{i,i} - e_{i,-i} - e_{-i,-i} - e_{-i,i} \in O(2l+1,k)$ *is a product of elementary matrices.*
(3) *The element* $w_{i,-i} = I - e_{i,-i} - e_{-i,i} - e_{i,i} - e_{-i,-i} \in O(2l,k)$ *is a product of elementary matrices.*

Proof. For the symplectic group $\mathrm{Sp}(2l,k)$ we have $w_{i,-i} = x_{i,-i}(1)x_{-i,i}(-1)x_{i,-i}(1)$. For the orthogonal group $\mathrm{O}(2l+1,k)$ we have $w_{i,-i} = x_{0,i}(-1)x_{i,0}(1)x_{0,i}(-1)$.

For the orthogonal group $\mathrm{O}(2l,k)$ we inductively produce these elements. First we get $w_{i,-j} = (I + e_{i,-j} - e_{j,-i})(I + e_{-i,j} - e_{-j,i})(I + e_{i,-j} - e_{j,-i}) = I - e_{i,i} - e_{j,j} - e_{-i,-i} - e_{-j,-j} + e_{i,-j} - e_{j,-i} + e_{-i,j} - e_{-j,i}$ and $w_{i,j} = I - e_{i,i} - e_{j,j} + e_{i,j} - e_{j,i} - e_{-i,-i} - e_{-j,-j} + e_{-i,-j} - e_{-j,-i}$. Now we set $w_{l,-l} = w_l$. Then compute $w_{(l-1),-(l-1)} = w_l w_{l,l-1} w_{l,-(l-1)} = I - e_{l-1,l-1} - e_{-(l-1),-(l-1)} - e_{(l-1),-(l-1)} - e_{-(l-1),(l-1)}$. •

Lemma 4.7. (1) *In the case of $Sp(2l,k)$, the element* $\mathrm{diag}(1,\ldots,1\lambda,1,\ldots,1,\lambda^{-1})$ *is a product of elementary matrices.*

(2) *In the case of $O(2l+1,k)$ the diagonal element* $\mathrm{diag}(-1,1,\ldots,1,\lambda^2,1,\ldots,1,\lambda^{-2})$ *is a product of elementary matrices.*

Proof. In the case of $\mathrm{Sp}(2l,k)$, we compute $w_{l,-l}(t) = (I+te_{l,-l})(I-t^{-1}e_{-l,l})(I+te_{l,-l}) = I-e_{l,l}-e_{-l,-l}+te_{l,-l}-t^{-1}e_{-l,l}$ and then compute $h_l(\lambda) = w_{l,-l}(\lambda)w_{l,-l}(-1)$ which is the required element.

In the case of $\mathrm{O}(2l+1,k)$ we compute $w_{l,0}(t) = x_{0,l}(-t)x_{l,0}(t^{-1})x_{0,l}(-t) = I-e_{-l,-l}-t^2e_{-l,l}-e_{l,l}-2e_{0,0}-t^{-2}e_{l,-l}$ and multiply it with $w_{l,0}(1)$ to get the required matrix. •

Remark : In the case of $\mathrm{O}(2l,k)$, the element $\mathrm{diag}(1,\ldots,1\lambda^2,1,\ldots,1,\lambda^{-2})$ and in the case of $\mathrm{O}(2l+1,k)$ the element $\mathrm{diag}(1,1,\ldots,1\lambda^2,1,\ldots,1,\lambda^{-2})$ is a product of elementary matrices.

Lemma 4.8. *Let* $g = \begin{pmatrix} \alpha & X & * \\ * & A & * \\ * & C & * \end{pmatrix}$ *be in $O(2l+1,k)$.*

(1) *If $A = \mathrm{diag}(1,\ldots,1,\lambda)$ and $X = 0$ then C is of the form* $\begin{pmatrix} C_{11} & -\lambda {}^TC_{21} \\ C_{21} & 0 \end{pmatrix}$ *with C_{11} skew-symmetric.*

(2) *If $A = \mathrm{diag}(1,\ldots,1,0,\ldots,0)$ with number of 1s equal $m < l$ and X has first m entries 0 then C is of the form* $\begin{pmatrix} C_{11} & 0 \\ * & * \end{pmatrix}$ *with C_{11} skew-symmetric.*

Proof. We use the equation ${}^Tg\beta g = \beta$ and get $2{}^TXX = -({}^TCA+{}^TAC)$. In the first case $X = 0$, so use 4.2 to get the required form for C. In the second case, we note that ${}^TXX$ has top-left block 0 and get the required form. •

Lemma 4.9. *Let* $g = \begin{pmatrix} \alpha & X & Y \\ * & A & * \\ * & 0 & D \end{pmatrix}$ *be in $O(2l+1,k)$ then $X = 0$ and $D = {}^TA^{-1}$.*

Proof. We compute ${}^Tg\beta g = \beta$ and get $2{}^TXX = 0$ and $2{}^TXY + {}^TAD = I$. This gives the required result. •

Lemma 4.10. *Let* $g = \begin{pmatrix} \alpha & 0 & Y \\ 0 & A & B \\ F & 0 & D \end{pmatrix}$*, with A an invertible diagonal matrix. Then, $g \in O(2l+1,k)$ if and only if $\alpha^2 = 1, F = 0 = Y$, $D = A^{-1}$ and ${}^TDB + {}^TBD = 0$.*

Proof.

$$\begin{aligned} {}^Tg\beta g &= \begin{pmatrix} \alpha & 0 & {}^TF \\ 0 & {}^TA & 0 \\ {}^TY & {}^TB & {}^TD \end{pmatrix} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & I \\ 0 & I & 0 \end{pmatrix} \begin{pmatrix} \alpha & 0 & Y \\ 0 & A & B \\ F & 0 & D \end{pmatrix} \\ &= \begin{pmatrix} 2\alpha^2 & {}^TFA & 2\alpha Y + {}^TFB \\ {}^TAF & 0 & {}^TAD \\ 2\alpha {}^TY + {}^TBF & {}^TDA & 2{}^TYY + {}^TDB + {}^TBD \end{pmatrix}. \end{aligned}$$

Equating this with β gives us the required result. •

5. Computing Spinor Norm for orthogonal groups

In this section, we show how we can use Gaussian elimination to compute spinor norm for orthogonal groups. The classical way to define spinor norm is via Clifford algebras [10, Chapters 8 & 9]. Spinor norm is a group homomorphism $\Theta\colon \mathrm{O}(d,k) \to k^\times/k^{\times 2}$, restriction of which to $\mathrm{SO}(d,k)$ gives $\Omega(d,k)$ as kernel. However, in practice, it is difficult to use that definition to compute the spinor norm. Wall [23], Zassenhaus [24] and Hahn [11] developed a theory to compute the spinor norm. For our exposition, we follow [22, Chapter 11].

Let g be an element of the orthogonal group. Consider g as a linear transformation. Futhermore, denote $\tilde{g} = I - g$ and $V_g = \tilde{g}(V)$ and $V^g = ker(\tilde{g})$. Using β we define Wall's bilinear form $[\ ,\ ]_g$ on V_g as follows:

$$[u,v]_g = \beta(u,y), \text{ where, } v = \tilde{g}(y).$$

This bilinear form satisfies following properties:

(1) $[u,v]_g + [v,u]_g = \beta(u,v)$ and $[u,u]_g = Q(u)$ for all $u,v \in V_g$.
(2) g is an isometry on V_g with respect to $[\ ,\ ]_g$.
(3) $[v,u]_g = -[u,gv]$ for all $u,v \in V_g$.
(4) $[\ ,\ ]_g$ is non-degenerate.

Then the **spinor norm** is

$$\Theta(g) = \overline{\mathrm{disc}(V_g, [\ ,\ ]_g)} \text{ if } g \neq I$$

extended to I by defining $\Theta(I) = \overline{1}$. An element g is called regular if V_g is non-degenerate subspace of V with respect to the form β. Hahn [11, Proposition 2.1] proved that for a regular element g the spinor norm is $\Theta(g) = \overline{\det(\tilde{g}|_{V_g})\mathrm{disc}(V_g)}$. This gives,

Proposition 5.1. (1) *For a reflection ρ_v, $\Theta(\rho_v) = \overline{Q(v)}$.*
(2) $\Theta(-1) = \overline{disc(V,\beta)}$.
(3) *For a unipotent element g the spinor norm is trivial, i.e., $\Theta(g) = \overline{1}$.*

Murray and Roney-Dougal [16] used the formula of Hahn to compute spinor norm. However, we show (Corollary B) that the Gaussian elimination developed in Section 4 ouptuts the spinor norm quickly. First we observe the following:

Lemma 5.2. *For the group $O(d,k)$, $d \geq 4$,*

(1) $\Theta(x_{i,j}(t)) = \Theta(x_{-i,j}(t)) = \Theta(x_{i,-j}(t)) = \overline{1}$. *Furthermore, in odd case we also have $\Theta(x_{i,0}(t)) = \overline{1} = \Theta(x_{0,i}(t))$.*
(2) $\Theta(w_l) = \overline{1}$.
(3) $\Theta(\mathrm{diag}(1,\ldots,1,\lambda,1,\ldots,1,\lambda^{-1})) = \overline{\lambda}$.

Proof. We use Proposition 5.1. The first claim follows from the fact that all elementary matrices are unipotent. The element $w_l = \rho_{(e_l+e_{-l})}$ is a reflection thus $\Theta(w_l) = \overline{Q(e_l+e_{-l})} = \overline{1}$.

For the third part we note that $\mathrm{diag}(1,\ldots,1,\lambda,1,\ldots,1,\lambda^{-1}) = \rho_{(e_l+e_{-l})}\rho_{(e_l+\lambda e_{-l})}$ and hence the spinor norm $\Theta(\mathrm{diag}(1,\ldots,1,\lambda,1,\ldots,1,\lambda^{-1})) = \Theta(\rho_{(e_l+\lambda e_{-l})}) = \overline{Q(e_l+\lambda e_{-l})} = \overline{\lambda}$. •

Proof of Corollary B. Let $g \in \mathrm{O}(d,k)$. From Theorem A, we write g as a product of elementary matrices and a diagonal matrix $\mathrm{diag}(1,\ldots,1,\lambda,1,\ldots,1,\lambda^{-1})$. Furthermore, the spinor norm of an elementary matrix is $\overline{1}$. Thus $\Theta(g) = \Theta(\mathrm{diag}(1,\ldots,1,\lambda,1,\ldots,1,\lambda^{-1})) = \overline{\lambda}$. •

6. Double coset decomposition for Siegel maximal parabolic

In this section, we compute the double coset decomposition with respect to Siegel maximal parabolic subgroup using our algorithm. Let P be the Siegel maximal parabolic of G where G is either $\mathrm{O}(d,k)$ or $\mathrm{Sp}(2l,k)$. In Lie theory, a parabolic is obtained by fixing a subset of

simple roots [4, Section 8.3]. Siegel maximal parabolic corresponds to the subset consisting of all but the last simple root. Geometrically, a parabolic subgroup is obtained as fixed subgroup of a totally isotropic flag [15, Proposition 12.13]. The Siegel maximal parabolic is the fixed subgroup of following isotropic flag (with the basis in Section 2):

$$\{0\} \subset \{e_1, \ldots, e_l\} \subset V.$$

Thus P is of the form $\begin{pmatrix} \alpha & 0 & Y \\ E & A & B \\ F & 0 & D \end{pmatrix}$ in $\mathrm{O}(2l+1,k)$ and $\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$ in $\mathrm{Sp}(2l,k)$ and $\mathrm{O}(2l,k)$.

The problem is to get the double coset decomposition $P\backslash G/P$. That is, we want to write $G = \bigsqcup_{\omega \in \hat{W}} P\omega P$ as disjoint union where $\hat{W}$ is a finite subset of G. Equivalently, given $g \in G$ we need an algorithm to determine the unique $\omega \in \hat{W}$ such that $g \in P\omega P$. If G is connected with Weyl group W and suppose W_P is the Weyl group corresponding to P then [5, Proposition 2.8.1]

$$P\backslash G/P \longleftrightarrow W_P\backslash W/W_P.$$

We need a slight variation of this as the orthogonal group is not connected.

In the case of $\mathrm{Sp}(2l,k)$, the Weyl group $W = N(T)/T$ where T is a diagonal maximal torus and $T = \{\mathrm{diag}(\lambda_1, \ldots, \lambda_l, \lambda_1^{-1}, \ldots, \lambda_l^{-1}) \mid \lambda_i \in k^\times\}$. The group W is isomorphic to a subgroup of S_{2l}, the symmetric group on $2l$ symbols $\{1, \ldots, l, -1, \ldots, -l\}$ and is generated by elements $w_{i,i+1}$ and $w_{i,-i}$ which map to permutations $(i,i+1)(-i,-(i+1))$ and $(i,-i)$ respectively. Thus W is isomorphic to $S_l \rtimes (\mathbb{Z}/2\mathbb{Z})^l$ and the subgroup W_P is generated by $w_{i,i+1}$ which proves that the subgroup $\{(i,i+1)(-i,-(i+1)) \mid 1 \le i \le l\}$ is isomorphic to S_l.

For $\mathrm{Sp}(2l,k)$, we set $\hat{W} = \{\omega_0 = I, \omega_i = w_{1,-1} \cdots w_{i,-i} \mid 1 \le i \le l\}$ and note that $W = \bigsqcup_{i=0}^{l} W_P \omega_i W_P$.

In the case of $\mathrm{O}(d,k)$, we set $\hat{W} = \{\omega_0 = I, \omega_i = w_{1,-1} \cdots w_{i,-i} \mid 1 \le i \le l\}$ where $w_{i,-i}$ is inductively produced (see Lemma 4.6).

Theorem 6.1. *Let P be the Siegel maximal parabolic subgroup in G, where G is either $O(d,k)$ or $Sp(d,k)$. Let $g \in G$. Then there is an efficient algorithm to determine ω such that $g \in P\omega P$. Furthermore, $\hat{W}$ the set of all ωs is a finite set of $l+1$ elements where $d = 2l$ or $2l+1$.*

Proof. In this proof we proceed with a similar but slightly different Gaussian elimination algorithm. Recall that $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ whenever g belongs to $\mathrm{Sp}(2l,k)$ or $\mathrm{O}(2l,k)$ or $g = \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix}$ whenever g belongs to $\mathrm{O}(2l+1,k)$. In our algorithm, we made A into a diagonal matrix. Instead of that, we can use elementary matrices ER1 and EC1 to make C into a diagonal matrix and then do the row interchange to make A into a diagonal matrix and C a zero matrix. If we do that, we note that elementary matrices E1 and E2 are in P. The proof is just keeping track of elements of P in this Gaussian elimination algorithm. The step 1 in the algorithm says that there are elements $p_1, p_2 \in P$ such that $p_1 g p_2 = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}$ where C_1 is a diagonal matrix with m non-zero entries. Clearly $m = 0$ if and only if $g \in P$. In that case g is in the double coset $P\omega_0 P = P$. Now suppose $m \ge 1$. Then in Step 2 we multiply by E2 to make the first m rows of A_1 zero, i.e., there is a $p_3 \in P$ such that $p_3 p_1 g p_2 = \begin{pmatrix} \tilde{A}_1 & \tilde{B}_1 \\ C_1 & D_1 \end{pmatrix}$ where first m rows of $\tilde{A}_1$ are zero. After this we interchange rows i with $-i$ for $1 \le i \le m$ which makes C_1 zero, i.e., multiplying by ω_m we get $\omega_m p_3 p_1 g p_2 = \begin{pmatrix} A_2 & B_2 \\ 0 & D_2 \end{pmatrix} \in P$. Thus $g \in P\omega_m P$.

For $O(2l+1,k)$ we note that the elementary matrices E1, E2 and E4a are in P. Rest of the proof is similar to the earlier case and follows by carefully keeping track of elementary matrices used in our algorithm in Section 4.2. •

7. CONCLUSIONS

We conclude this paper with some implementation results of our algorithm and some comparisons with an existing algorithm. Before we state those, we wander a little towards a direction for further research. Chevalley generators are known for a long time. However, its use in row-column operations is new. Earlier, in computational group theory, while working with quasisimple groups, the generators of choice were always the standard generators. This use of Chevalley generaotrs can bring in a paradigm shift with algorithms in matrix groups. It is now a very interesting project to redo the constructive group recognition project [13] with our algorithms and Chevalley generators.

Now some implementation results, we implemented our algorithm in magma [2]. We found our implementation to be fast and stable. In magma, Costi and C. Schneider installed a function *ClassicalRewriteNatural*. It is the row-column operation developed by Costi [8] in natural representation. We tested the time taken by our algorithm and the one taken by the Magma function. To do this test, we followed Costi [8, Table 6.1] as closely as possible. Two kind of simulations were done. In one case, we fixed the size of the field at 7^{10} and varied the size of the matrix from 20 to 60. To time both these algorithms for any particular input, we took one thousand random samples from the group and run the algorithm for each one of them. Then the final time was the average of this one thousand random repetitions. The times were tabulated and presented below.

In the other case, we kept the size of the matrix fixed at 20 and we varied the size of the field, keeping the characteristic fixed at 7. In many cases the magma computation for the function ClassicalRewriteNatural will not stop in a reasonable amount of time or will give an error and not finish computing. In those cases, though our algorithm worked perfectly, we were unable to get adequate data to plot and are represented by gaps in the graph drawn. Here also the times are the average of one thousand random repetitions. It seems that our algorithms perform

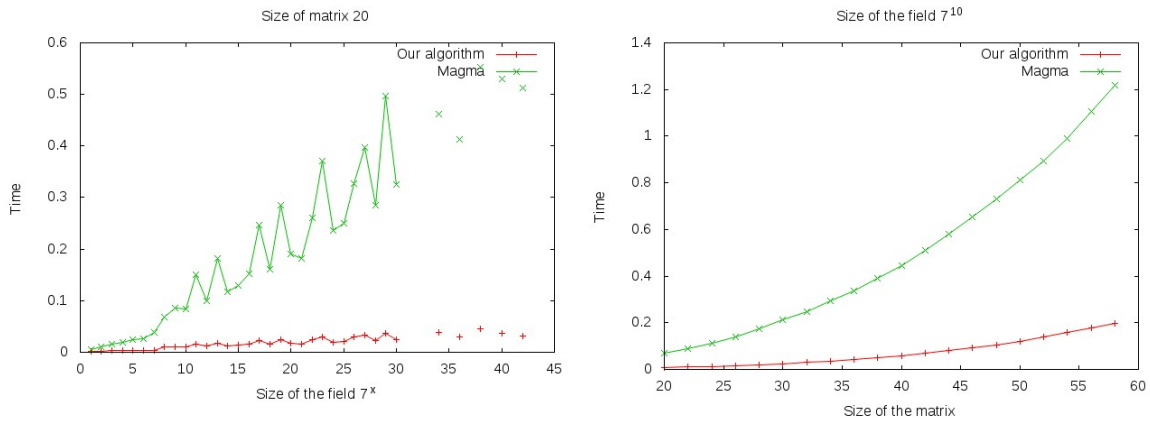

FIGURE 1. Some simulations comparing our algorithm with the one inbuilt in Magma for even-order orthogonal groups

better than that of Costi's on all fronts.

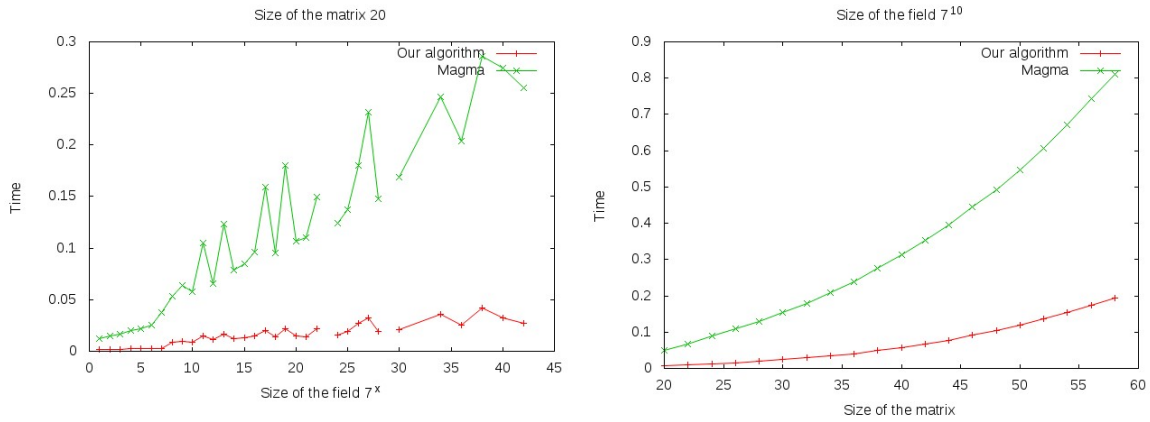

FIGURE 2. Some simulations comparing our algorithm with the one inbuilt in Magma for symplectic groups

REFERENCES

1. S. Ambrose, S. Murray, C. E. Praeger, and C. Schneider, *Constructive membership testing in black-box classical groups*, Proceedings of The Third International Congress on Mathematical Software, LNCS, vol. 6327, 2011, pp. 54–57.
2. Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).
3. Peter Brooksbank, *Constructive recognition of classical groups in their natural representation*, Journal of Symbolic Computation **35** (2003), 195–239.
4. Roger Carter, *Simple groups of Lie type*, Pure and Applied Mathematics, vol. 28, John Wiley & Sons, 1972.
5. _____, *Finite groups of Lie type*, John Wiley & Sons, 1993.
6. C. Chevalley, *Sur certains groupes simples*, Tohoku Math. J. **7** (1955), no. 2, 14–66.
7. Arjeh M. Cohen, Scott H. Murray, and D. E. Taylor, *Computing in groups of Lie type*, Mathematics of computation **73** (2003), no. 247, 1477–1498.
8. Elliot Costi, *Constructive membership testing in classical groups*, Ph.D. thesis, Queen Mary, Univ. of London, 2009.
9. Joseph F. Grcar, *Mathematicians of Gaussian elimination*, Notices of the AMS **58** (2011), no. 6, 782–792.
10. Larry C. Grove, *Classical groups and geometric algebra*, vol. 39, American Mathematical Society, Graduate Studies in Mathematics, 2002.
11. Alexander J. Hahn, *Unipotent elements and the spinor norms of Wall and Zassenhaus*, Arch. Math. (Basel) **32** (1979), no. 2, 114–122.
12. William Kantor and Àkos Seress, *Black box classical groups*, vol. 149, Memoirs of the American Mathematical Society, 2001.
13. C. R. Leedham-Green and E. A. O'Brien, *Constructive recognition of classical groups in odd characteristic*, J. Algebra **322** (2009), no. 3, 833–881.
14. Ayan Mahalanobis and Anupam Singh, *Gaussian elimination in unitary groups with an application to cryptography*, Tech. report, IISER Pune, 2015, http://arxiv.org/pdf/1409.6136.pdf.
15. Gunter Malle and Donna Testerman, *Linear algebraic groups and finite groups of lie type*, Cambridge University Press, 2011.
16. Scott H. Murray and Colva M. Roney-Dougal, *Constructive homomorphisms for classical groups*, Journal of Symbolic Computation **46** (2011), 371–384.
17. Alice C. Niemeyer and Cheryl E. Praeger, *A recognition algorithm for classical groups over finite fields*, Proceedings of the London Mathematical Society **77** (1998), no. 3, 117–169.
18. E. A. O'Brien, *Algorithms for matrix groups*, Groups St Andrews 2009 in Bath, Volume 2, London Math. Soc. Lecture Note Ser., vol. 388, Cambridge Univ. Press, 2011, pp. 297–323.
19. E. A. O'Brien, *Towards effective algorithms for linear groups*, Proceedings of the Conference 'Finite Geometries, Groups, and Computation', Colorado, 2004, pp. 163–190.
20. Ákos Seress, *An introduction to computational group theory*, Notices of the AMS **44** (1997), no. 6, 671–679.
21. Robert Steinberg, *Lectures on Chevalley groups. notes prepared by John Faulkner and Robert Wilson*, Yale University, 1968.

22. Donald E. Taylor, *The geometry of the classical groups*, Heldermann Verlag, 1992.
23. G. E. Wall, *The structure of a unitary factor group*, Inst. Hautes Études Sci. Publ. Math (1959), no. 1, 23 pp.
24. Hans Zassenhaus, *On the spinor norm*, Arch. Math. (1962), no. 13, 434–451.